

# PATENT ABSTRACTS OF JAPAN

00/8119  
ISR 314811  
(3)

(11)Publication number : 10-282883

(43)Date of publication of application : 23.10.1998

(51)Int.Cl. G09C 1/00  
G06F 13/00  
H04L 9/32

(21)Application number : 09-089774

(71)Applicant : OKI ELECTRIC IND CO LTD

(22)Date of filing : 08.04.1997

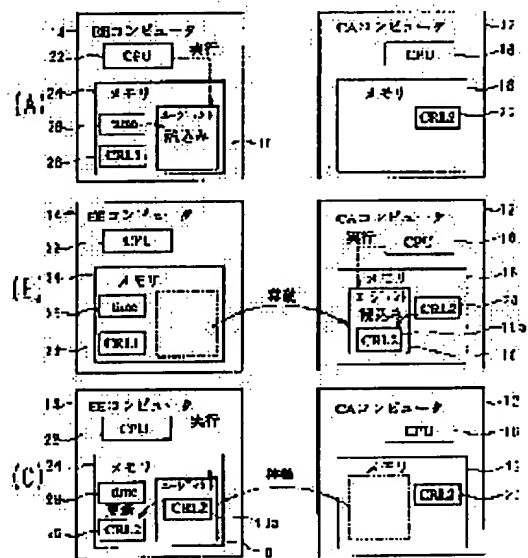
(72)Inventor : MORI TAKESHI

## (54) METHOD FOR DISTRIBUTING INEFFECTIVE DIGITAL CERTIFICATE LIST

### (57)Abstract:

**PROBLEM TO BE SOLVED:** To provide the distributing method for CRL(ineffective digital certificate list) which can reduce the load of the designing of an application system and the system of an authentication office.

**SOLUTION:** An agent program 10 for a processing procedure for distributing CRL is used. This agent program 10 moves to the authentication office 12 according to its program. Then the latest CRL which is issued by the authentication office 12 is read in an authentication office memory 18. The agent program 10 moves to a terminal memory 24 together with the latest CRL according to its program. Then the CRL of a terminal entity 14 is updated into the latest CRL.



## LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平10-282883

(43) 公開日 平成10年(1998)10月23日

(51) Int.Cl.<sup>8</sup>

G 0 9 C 1/00

G 0 6 F 13/00

H 0 4 L 9/32

識別記号

6 4 0

3 5 1

F I

G 0 9 C 1/00

G 0 6 F 13/00

H 0 4 L 9/00

6 4 0 B

3 5 1 E

6 7 5 D

審査請求 未請求 請求項の数4 O L (全 14 頁)

(21) 出願番号

特願平9-89774

(22) 出願日

平成9年(1997)4月8日

(71) 出願人 000000295

沖電気工業株式会社

東京都港区虎ノ門1丁目7番12号

(72) 発明者 森 健

東京都港区虎ノ門1丁目7番12号 沖電気  
工業株式会社内

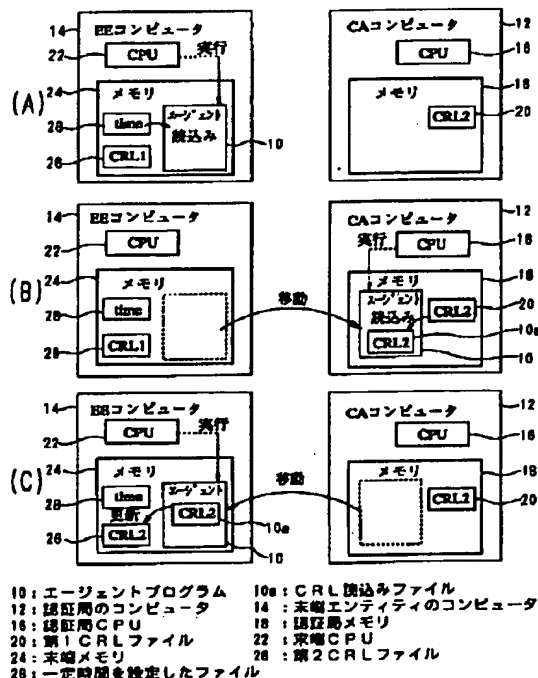
(74) 代理人 弁理士 大垣 孝

(54) 【発明の名称】 無効デジタル証明書リストの配布方法

(57) 【要約】

【課題】 アプリケーションシステムや認証局のシステムの設計の負荷を低減することができるCRLの配布方法の提供。

【解決手段】 CRLを配布するための処理手順がプログラムされたエージェントプログラム10を用いる。このエージェントプログラム10は、自身のプログラムに従って認証局12へ移動する。次に、認証局メモリ18に、認証局の発行している最新のCRLを読み込む。一定時間の経過後に、エージェントプログラム10は、自身のプログラムに従って、最新のCRLを携えて、末端メモリ24に移動する。そして、末端エンティティ14のCRLを最新のCRLに更新する。



第1の実施の形態のブロック図

## 【特許請求の範囲】

【請求項1】 末端エンティティのコンピュータの記憶装置（以下、「末端メモリ」とも称する。）に、無効デジタル証明書リストを配布するための処理手順がプログラムされたエージェントプログラムを格納しておき、末端エンティティのコンピュータの中央演算装置（以下、「末端CPU」とも称する。）によって、前記エージェントプログラムを起動し、

前記末端CPUによって前記エージェントプログラムを実行することにより、前記エージェントプログラムを認証局のコンピュータの記憶装置（以下「認証局メモリ」とも称する。）に格納し、

前記認証局のコンピュータの中央演算装置（以下、「認証局CPU」とも称する。）によって前記エージェントプログラムを実行することにより、前記認証局メモリのうちの当該エージェントプログラムが使用するメモリ領域に、前記認証局の発行している最新の無効デジタル証明書リストを格納し、かつ、一定時間の経過後に、前記エージェントプログラムを前記メモリ領域に格納された最新の無効デジタル証明書リストと共に前記末端メモリに格納し、

前記末端CPUによって前記エージェントプログラムを実行することにより、前記末端メモリに格納されている無効デジタル証明書リストを前記最新の無効デジタル証明書リストに更新することを特徴とする無効デジタル証明書リストの配布方法。

【請求項2】 請求項1に記載の無効デジタル証明書リストの配布方法において、

前記一定時間を前記末端メモリに格納しておき、前記エージェントプログラムが前記認証局のメモリに格納される前に、前記末端CPUによって前記エージェントプログラムを実行することにより、当該一定時間を前記末端メモリから当該エージェントプログラムに読込むことを特徴とする無効デジタル証明書リストの配布方法。

【請求項3】 認証局のコンピュータの記憶装置（以下、「認証局メモリ」とも称する。）に、無効デジタル証明書リストを配布するための処理手順がプログラムされたエージェントプログラムを格納しておき、前記認証局のコンピュータの中央演算装置（以下、「認証局CPU」とも称する。）によって、前記エージェントプログラムを起動し、

前記認証局CPUによって前記エージェントプログラムを実行することにより、前記認証局メモリのうちの当該エージェントプログラムが使用するメモリ領域に、前記認証局の発行している最新の無効デジタル証明書リストを格納し、かつ、前記エージェントプログラムを前記メモリ領域に格納された最新の無効デジタル証明書リストと共に末端エンティティのコンピュータの記憶装置（以下、「末端メモリ」とも称する。）に格納し、

前記末端エンティティのコンピュータの中央演算装置によって前記エージェントプログラムを実行することにより、当該末端メモリに格納されている無効デジタル証明書リストを前記最新の無効デジタル証明書リストに更新し、かつ、更新後に、前記エージェントプログラムを前記認証局メモリに格納することを特徴とする無効デジタル証明書リストの配布方法。

【請求項4】 第1の認証局のコンピュータの記憶装置（以下、「第1認証局メモリ」とも称する。）に、無効デジタル証明書リストを配布するための処理手順がプログラムされたエージェントプログラムを格納しておき、

前記第1の認証局のコンピュータの中央演算装置（以下、「第1認証局CPU」とも称する。）によって、前記エージェントプログラムをそれぞれ起動し、

前記第1認証局CPUによって前記エージェントプログラムを実行することにより、前記第1認証局メモリのうちの当該エージェントプログラムが使用するメモリ領域に、前記第1認証局の発行している最新の無効デジタル証明書リストを格納し、かつ、前記エージェントプログラムを前記メモリ領域に格納された最新の無効デジタル証明書リストと共に第2の認証局のコンピュータの記憶装置（以下、「第2認証局メモリ」とも称する。）に格納し、

前記第2の認証局のコンピュータの中央演算装置によって前記エージェントプログラムを実行することにより、当該第2認証局メモリに格納されている、前記第1認証局によって発行された無効デジタル証明書リストを前記最新の無効デジタル証明書リストに更新し、かつ、更新後に、前記エージェントプログラムを前記第1認証局メモリに格納することを特徴とする無効デジタル証明書リストの配布方法。

## 【発明の詳細な説明】

【0001】

【発明の属する技術分野】この発明は、ITU-T（国際電気通信連合 電気通信標準化部門）勧告X.509「ディレクトリー認証の枠組み」に準拠した認証局（証明書発行局（Certification Authority；CA））が、無効となったデジタル証明書のリストを各ユーザ等の末端エンティティ（End Entity；EE）に配布するための方法に関する。

【0002】

【従来の技術】インターネットのようなオープンネットワークシステムにおいて、例えば電子商取引（Electric Commerce；EC）といったシステムを実現するためには、ユーザの認証（身元保証）を行うこと、および、通信メッセージの機密性の確保および改竄の防止（正当性の保持）を行うことが不可欠である。このため、公開鍵暗号を利用した認証および暗号化方式の一例が、文献：「ソフトウェアデザイン、1996年11月号、pp.

72-89」に「エレクトロニックコマースとセキュリティ」と題して記載されている。この方式においては、ユーザの認証のために、デジタル証明書（電子印鑑証明書）が用いられる。このデジタル証明書は、ユーザの公開鍵を含み、その鍵が正しく当該ユーザの公開鍵であることを保証するものである。そして、このデジタル証明書は、ITU-T勧告X.509に準拠した認証局によって発行される。

#### 【0003】

【発明が解決しようとする課題】認証局は、一定の有効期限が経過したり、証明書に関する鍵ペアの暗号が漏洩した等の理由によって、発行されたデジタル証明書を破棄または更新することにより無効とすることがある。そして、認証局は、上述のITU-T勧告X.509に準拠した無効となったデジタル証明書のリスト（以下、「無効デジタル証明書リスト」とも称し、「CRL」とも表記する。）を作成して管理する必要がある。そして、このCRLは、各ユーザに配布される必要がある。

【0004】しかしながら、CRLの配布にあたり、次のような問題点がある。

【0005】先ず、認証局（CA）から末端エンティティ（EE）へCRLを配布するためには、オープンネットワークシステムにおいて実現されるアプリケーションシステムを設計する際に、CRLの配布を実現するためのメッセージやプロトコルといった仕組みを一緒に設計する必要がある。

【0006】ところが、CRLを配布するための仕組みと、個々のアプリケーション（AP）システムとでは、設計のレベルが異なる。ここでレベルが異なるとは、アプリケーションシステムにおいては、個々のアプリケーションシステムに応じたメッセージやプロトコルといった仕組みを設計する必要がある（例えば、電子商取引のアプリケーションシステムにおいては、客、店および金融機関の間で、相手の確認や金銭のやり取りを行うためのメッセージやプロトコルを設計する必要がある。）のに対して、ITU-T勧告X.509に準拠したCRLを配布するための仕組みにおいては、個々のアプリケーションシステムの種類に依存しないより基本的なレベルでの仕組みを設計する必要があることをいう。

【0007】このようにレベルが異なるため、CRLを配布するための仕組みの設計は、アプリケーションシステムを設計する上で大きな負担となる。

【0008】また、CRLの内容は、認証局において運用上定められた一定時間毎に更新される。一方、CRLの配布の時間間隔は、アプリケーションシステムによって異なる。その結果、末端エンティティが保持しているCRLと、認証局が保持している最新のCRLとの間に時間的なずれが生じる。そして、更新および配布の時間間隔の設定が悪い場合には、この時間的なずれが大きく

なる。その場合、末端エンティティが保持しているCRLの信頼度が低下してしまう。このため、CRLの信頼度の低下を防ぐためには、CRLの更新の時間間隔に対するCRLの配布の時間間隔を最適に設定することが求められる。

【0009】ところが、アプリケーションシステムの設計に、CRLの配布の仕組みが組み込まれている場合には、CRLの配布の時間間隔を簡単には変更できない。ここで、CRLの配布の仕組みが組み込まれている場合とは、例えば、個々のアプリケーションシステムに応じたメッセージのやり取りと同時にCRLの配布を行うように設計してある場合である。より具体的な例としては、電子商取引において店から金融機関への送金を行うのと同時にCRLの配布を行うように設計してあるような場合である。この場合、送金が1日に1回だけの場合（通信費を節約したい場合や、夜間に1回、その日の売上を金融機関に送れば送金頻度が十分な場合が考えられる。）には、CRLの配布も1日に1回だけとなる。そして、店が客の身元をより正確に確認するためにより頻繁なCRLの配布を希望しても、送金頻度を変更せずにCRLの配布の時間間隔だけを後から変更することは困難である。

【0010】また、複数の認証局（CA）どうしが協調して動作する、より大きなシステムを構築する場合には、認証局どうしの間で互いにCRLを配布し合う仕組みが必要となる。ここで、認証局どうしが協調して動作するとは、互いに異なる認証局がそれぞれ発行したデジタル証明書を、互いに信用して良いという取り決めをしている場合をいう。このように、認証局どうしが協調して動作すれば、互いに異なる認証局によってそれぞれ認証（身元保証）された末端エンティティのユーザどうしが、互いに相手を信用することができる。これに対して、認証局が協調して動作しない場合には、互いに異なる認証局からデジタル証明書を付与された末端エンティティのユーザどうしは、通常、相手のデジタル証明書を信用することができない。

【0011】ところが、既に一つの認証局が稼働しているシステムに、後から他の認証局からのCRLの配布の仕組みを組み入れるためには、システムの設計を大きく変更する必要がある。このため、複数の認証局どうしを後から協調して動作させることは、システムの設計の上で大きな負担となる。

【0012】このため、アプリケーションシステムや認証局のシステムの設計の負荷を低減することができる新規なCRLの配布方法の実現が望まれていた。

#### 【0013】

【課題を解決するための手段】そこで、この出願に係る発明者は、種々の検討を重ねた結果、アプリケーションシステムや認証局のシステム自体に無効デジタル証明書リスト（CRL）の配布の仕組みを設計するのではな

10

20

30

40

50

く、CRLを配布するための処理手順がプログラムされたエージェントプログラムを用いることを考えた。

【0014】[第1の無効デジタル証明書リストの配布方法について]この発明の第1の無効デジタル証明書リスト(CRL)の配布方法によれば、末端エンティティのコンピュータの記憶装置(末端メモリ)に、CRLを配布するための処理手順がプログラムされたエージェントプログラムを格納しておき、末端エンティティのコンピュータの中央演算装置(末端CPU)によって、エージェントプログラムを起動し、末端CPUによってエージェントプログラムを実行することにより、エージェントプログラムを認証局のコンピュータの記憶装置

(認証局メモリ)に格納し、認証局のコンピュータの中央演算装置(認証局CPU)によってエージェントプログラムを実行することにより、認証局メモリのうちのこのエージェントプログラムが使用するメモリ領域に、認証局の発行している最新のCRLを格納し、かつ、一定時間の経過後に、エージェントプログラムをメモリ領域に格納された最新のCRLと共に末端メモリに格納し、末端CPUによってエージェントプログラムを実行することにより、末端メモリに格納されているCRLを最新のCRLに更新することを特徴とする。

【0015】このように、この発明の第1の無効デジタル証明書の配布方法によれば、CRLを配布するための処理手順がプログラムされたエージェントプログラムを用いる。

【0016】そして、第1の無効デジタル証明書リストの配布方法によれば、CRLの配布を行うにあたり、まず、末端メモリに格納されていたエージェントプログラムを末端CPUによって起動する。すなわち、末端CPUによってエージェントプログラムの実行を開始する。

【0017】次に、末端CPUによってエージェントプログラムを実行することにより、エージェントプログラム自身は、認証局メモリに、オープンネットワークシステムを介して送られて格納される。すなわち、エージェントプログラムは、自身のプログラムに従って認証局へ移動する。

【0018】次に、認証局メモリに格納されたエージェントプログラムは、認証局CPUによって実行される。その結果、エージェントプログラムの処理手順に従って、認証局メモリのうちのこのエージェントプログラムが使用するメモリ領域に、認証局の発行している最新のCRLが格納される。

【0019】そして、エージェントプログラムは、一定時間、認証局メモリに格納されている。すなわち、エージェントプログラムは、一定時間、認証局に駐在する。また、エージェントプログラムが認証局に駐在している間に認証局のCRLが更新された場合には、更新されたCRLが最新のCRLとなるが、エージェントプログラ

ムでCRLの更新を監視し、この更新されたCRLをメモリ領域に新たに格納する。

【0020】そして、一定時間の経過後に、エージェントプログラムは、メモリ領域に格納された最新のCRLと共に末端メモリに、オープンネットワークシステムを介して送られて格納される。すなわち、エージェントプログラムは、自身のプログラムに従って、最新のCRLを携えて、末端メモリに移動する。

【0021】次に、末端メモリに格納されたエージェントプログラムは、末端CPUによって実行される。その結果、エージェントプログラムの処理手順に従って、末端メモリに格納されている古いCRLは、戻ったエージェントプログラムが持ち帰った最新のCRLに更新される。このようにして、エージェントプログラムにより認証局から末端エンティティへCRLが配布される。

【0022】このように、この発明の第1の無効デジタル証明書リストの配布方法によれば、エージェントプログラムを用いる。そして、このエージェントプログラムにCRLの配布の仕組みの処理手順を設計する。その結果、アプリケーションシステムの設計をCRLの配布の仕組みの設計から切り離して行うことができる。このため、アプリケーションシステムの設計の負担を軽減することができる。

【0023】また、この発明の第1の無効デジタル証明書リストの配布方法を実施するにあたり、好ましくは、一定時間を末端メモリに格納しておき、エージェントプログラムが認証局のメモリに格納される前に、末端CPUによってエージェントプログラムを実行することにより、この一定時間を末端メモリから当該エージェントプログラムに読込むと良い。

【0024】このように、末端メモリに格納しておいた一定時間をエージェントプログラムに読み込ませて設定すれば、末端メモリに所望の値の一定時間を格納しておくことにより、エージェントプログラムが認証局に駐在している時間の長さを所望の長さとすることができる。その結果、エージェントプログラムが認証局から末端エンティティに戻ってくるタイミングを所望のタイミングとすることができる。このため、CRLの配布による末端エンティティのCRLの更新のタイミングを所望のタイミングとすることができる。

【0025】[第2の無効デジタル証明書リストの配布方法について]ところで、第1の無効デジタル証明書リストの配布方法によれば、エージェントプログラムが、一定時間、認証局に駐在する。そして、駐在している間、エージェントプログラムは、認証局のコンピュータの中央演算装置(認証局CPU)によって実行される。また、エージェントプログラムは、認証局に駐在している間、認証局のコンピュータの記憶装置(認証局メモリ)の記憶容量のうちの一部分のメモリ領域を占有している。このため、認証局にエージェントプログラムが

駐在している間、認証局のコンピュータの負担が大きくなる。

【0026】ところが、認証局のコンピュータの演算能力および記憶容量といった処理能力は、一般に、余裕が少ない。その上、多数の末端エンティティから多数のエージェントプログラムが認証局に駐在すると、認証局のコンピュータの負担が非常に大きくなる。その結果、認証局自身の処理が滞るおそれがある。例えば、認証局によるCRLの発行に時間がかかってしまうおそれがある。

【0027】そこで、認証局のコンピュータの負担の増大を抑制するため、この発明の第2の無効デジタル証明書リストの配布方法によれば、認証局のコンピュータの記憶装置（認証局メモリ）に、無効デジタル証明書リストを配布するための処理手順がプログラムされたエージェントプログラムを格納しておき、認証局のコンピュータの中央演算装置（認証局CPU）によって、エージェントプログラムを起動し、認証局CPUによってエージェントプログラムを実行することにより、認証局メモリのうちのこのエージェントプログラムが使用するメモリ領域に、認証局の発行している最新の無効デジタル証明書リストを格納し、かつ、エージェントプログラムをメモリ領域に格納された最新の無効デジタル証明書リストと共に末端エンティティのコンピュータの記憶装置（末端メモリ）に格納し、末端エンティティのコンピュータの中央演算装置（以下、「末端CPU」とも称する。）によってエージェントプログラムを実行することにより、当該末端メモリに格納されている無効デジタル証明書リストを最新の無効デジタル証明書リストに更新し、かつ、更新後に、エージェントプログラムを認証局メモリに格納することを特徴とする。

【0028】このように、この発明の第2の無効デジタル証明書の配布方法によれば、CRLを配布するための処理手順がプログラムされたエージェントプログラムを用いる。

【0029】そして、第2の無効デジタル証明書リストの配布方法によれば、CRLの配布を行うにあたり、まず、認証局メモリに格納されていたエージェントプログラムを認証局CPUによって起動する。すなわち、認証局CPUによってエージェントプログラムの実行を開始する。

【0030】次に、認証局CPUによってエージェントプログラムを実行することにより、認証局メモリのうちのこのエージェントプログラムが使用するメモリ領域に、認証局の発行している最新の無効デジタル証明書リストが格納される。

【0031】そして、エージェントプログラム自身は、メモリ領域に格納された最新の無効デジタル証明書リストと共に、オープンネットワークシステムを介して送られて末端メモリに格納される。すなわち、エージェン

トプログラムは、自身のプログラムに従って末端エンティティへ移動する。

【0032】次に、末端メモリに格納されたエージェントプログラムは、末端CPUによって実行される。その結果、エージェントプログラムの処理手順に従って、当該末端メモリに格納されている古い無効デジタル証明書リストは、最新の無効デジタル証明書リストに更新される。このようにして、エージェントプログラムにより認証局から末端エンティティへCRLが配布される。

10 【0033】そして、CRLの更新後に、エージェントプログラムは、認証局メモリに、オープンネットワークシステムを介して送られて格納される。すなわち、エージェントプログラムは、自身のプログラムに従って、認証局メモリに移動する。

20 【0034】このように、この発明の第2の無効デジタル証明書リストの配布方法によれば、エージェントプログラムを用いる。そして、このエージェントプログラムにCRLの配布の仕組みの処理手順を設計する。その結果、アプリケーションシステムの設計をCRLの配布の仕組みの設計から切り離して行うことができる。このため、アプリケーションシステムの設計の負担を軽減することができる。

30 【0035】さらに、この発明の第2の無効デジタル証明書リストの配布方法によれば、認証局CPUによって、エージェントプログラムを起動して、エージェントプログラムを末端メモリへ移動させる。このため、第2の無効デジタル証明書リストの配布方法によれば、認証局へ末端エンティティからエージェントプログラムが殺到することがない。その結果、認証局のコンピュータの負担の増大を抑制することができる。従って、第2の無効デジタル証明書リストの配布方法は、特に認証局のコンピュータの処理能力に余裕がない場合に適用して好適である。

40 【0036】〔第3の無効デジタル証明書リストの配布方法について〕また、複数の認証局が協調して動作するシステムを構築する場合には、複数の認証局がそれぞれ発行したCRLを互いに配布する仕組みが必要となる。しかし、既存の認証局どうしを、後から協調して動作させるためには、従来は、システムの大きな変更が必要であった。

50 【0037】そこで、認証局のシステムを大きく変更せずに、認証局どうしを協調して動作させるために、この発明の第3の無効デジタル証明書リストの配布方法によれば、第1の認証局のコンピュータの記憶装置（以下、「第1認証局メモリ」とも称する。）に、無効デジタル証明書リストを配布するための処理手順がプログラムされたエージェントプログラムを格納しておき、第1の認証局のコンピュータの中央演算装置（以下、「第1認証局CPU」とも称する。）によって、エージェントプログラムをそれぞれ起動し、第1認証局CPUによ

ってエージェントプログラムを実行することにより、第1認証局メモリのうちのこのエージェントプログラムが使用するメモリ領域に、第1認証局の発行している最新の無効デジタル証明書リストを格納し、かつ、エージェントプログラムをメモリ領域に格納された最新の無効デジタル証明書リストと共に第2の認証局のコンピュータの記憶装置（以下、「第2認証局メモリ」とも称する。）に格納し、第2の認証局のコンピュータの中央演算装置（以下、「第2認証局CPU」とも称する。）によってエージェントプログラムを実行することにより、当該第2認証局メモリに格納されている、第1認証局によって以前に発行された無効デジタル証明書リストを最新の無効デジタル証明書リストに更新し、かつ、更新後に、エージェントプログラムを第1認証局メモリに格納することを特徴とする。

【0038】このように、この発明の第3の無効デジタル証明書リストの配布方法によれば、CRLを配布するための処理手順がプログラムされたエージェントプログラムを用いる。

【0039】そして、第3の無効デジタル証明書リストの配布方法によれば、第1認証局から第2認証局へCRLの配布を行うにあたり、先ず、第1認証局メモリに格納されていたエージェントプログラムを第1認証局CPUによって起動する。すなわち、第1認証局CPUによってエージェントプログラムの実行を開始する。

【0040】次に、第1認証局CPUによってエージェントプログラムを実行することにより、第1認証局メモリのうちのこのエージェントプログラムが使用するメモリ領域に、第1認証局の発行している最新の無効デジタル証明書リストが格納される。

【0041】そして、エージェントプログラム自身は、メモリ領域に格納された最新の無効デジタル証明書リストと共に、オープンネットワークシステムを介して送られて第2認証局メモリに格納される。すなわち、エージェントプログラムは、自身のプログラムに従って第2認証局へ移動する。

【0042】次に、第2認証局メモリに格納されたエージェントプログラムは、第2認証局CPUによって実行される。その結果、エージェントプログラムの処理手順に従って、当該第2認証局メモリに格納されている、第1認証局によって以前に発行された古い無効デジタル証明書リストは、最新の無効デジタル証明書リストに更新される。このようにして、エージェントプログラムにより第1認証局から第2認証局へCRLが配布される。

【0043】そして、CRLの更新後に、エージェントプログラムは、第1認証局メモリに、オープンネットワークシステムを介して送られて格納される。すなわち、エージェントプログラムは、自身のプログラムに従って、第1認証局メモリに移動する。

【0044】このように、この発明の第3の無効デジタル証明書リストの配布方法によれば、エージェントプログラムを用いる。そして、このエージェントプログラムにCRLの配布の仕組みの処理手順を設計する。その結果、個々の認証局のシステムの設計をCRLの配布の仕組みの設計から切り離して行うことができる。このため、認証局のシステムの設計の負担を軽減することができる。

【0045】また、第2認証局から第1認証局へCRLを配布する場合も、第1認証局から第2認証局へCRLを配布する場合と同様にしてCRLを配布することができる。さらに、第1認証局から第2認証局へCRLを配布する場合の処理手順を繰返すことによって、3つ以上の認証局どうしの間でCRLを互いに配布することも可能である。

【0046】

【発明の実施の形態】以下、図を参照して、この発明の第1～第3の無効デジタル証明書リストの配布方法の例についてそれぞれ説明する。

【0047】[第1の実施の形態] 第1の実施の形態では、図1および図2を参照して、この発明の第1の無効デジタル証明書リスト（CRL）の配布方法の一例について説明する。

【0048】図1の（A）～（C）は、第1の実施の形態のCRLの配布方法の説明に供するブロック図である。また、図2は、第1の実施の形態のCRLの配布方法の説明に供するフローチャートである。

【0049】先ず、CRLを配布するための処理手順がプログラムされたエージェントプログラム（以下、単に「エージェント」とも称する。）10が稼働する環境について説明する。通常は、認証局から多数の末端エンティティへCRLが配布されるが、ここでは、1つの末端エンティティおよび認証局に注目してCRLの配布方法について説明する。

【0050】図1に、認証局のコンピュータ（「CAコンピュータ」または「認証局」とも表記する。）12と、末端エンティティのコンピュータ（「EEコンピュータ」または「末端エンティティ」とも称する。）14を示す。認証局12と末端エンティティ14とは、互いにオープンネットワークシステムによって接続してある。また、認証局12および末端エンティティ14は、いずれも、エージェント10が動作可能な環境を有している。動作可能な環境とは、例えば、認証局12と末端エンティティ14との間でエージェント10の受渡が可能状態をいう。

【0051】また、認証局12は、認証局CPU16および認証局メモリ18を具えている。この認証局メモリ18には、この認証局が発行した最新の無効デジタル証明書リスト（CRL）が第1CRLファイル20として格納されている。第1の実施の形態においては、第1



CRLファイル20に、最新のCRLとして「CRL 2」を格納してある。

【0052】また、末端エンティティ14は、末端CPU22および末端メモリ24を具えている。この末端メモリ24には、認証局から配布されたCRLを格納するための第2CRLファイル26が格納されている。ここでは、第2CRLファイルに、以前に認証局12から配布された「CRL1」を古いCRLとして格納してある（図1の（A））。

【0053】尚、第2CRLファイル26の内容が、第1CRLファイル20の内容と同じ場合もあり得る。また、末端メモリ24には、エージェントを認証局に駐在させる一定時間を設定したファイル28が格納してある。

【0054】そして、末端メモリ24には、エージェントプログラム10がコンパイルされた状態で格納してある（図1の（A））。

【0055】尚、ここでは、認証局メモリ18や末端メモリ24といったコンピュータの記憶装置は、コンピュータに内蔵されているものに限定する必要はなく、例えば、コンピュータに接続された外部記憶装置、例えば、ハードディスク装置を用いても良い。

【0056】次に、第1の実施の形態におけるCRLの配布方法について説明する。

【0057】CRLの配布を行うにあたり、先ず、末端メモリ24に格納されていたエージェント10を末端CPU22によって起動する（図2のS1）。すなわち、末端CPU22によってエージェントプログラム10の実行を開始する。起動にあたっては、例えば、末端メモリ24中に格納されているローカルな関数の呼び出しを末端CPU22によって行うことによって、エージェント10の実行を開始させると良い。

【0058】次に、末端CPU22によってエージェントプログラム10を実行することにより、当該エージェントプログラム10に一定時間を読み込む（図2のS2）。一定時間の読み込みにあたっては、末端メモリ24に格納しておいた一定時間を設定したファイル28に格納された一定時間をエージェントプログラム10に読み込む。すなわち、エージェントプログラム10は、起動されると、先ずファイル28に格納した一定時間を読み込むようプログラムされている。

【0059】従って、このファイル28に、所望の値の一定時間（例えば、何分、何時間もしくは何日間という設定）を格納しておくことにより、エージェントプログラムが認証局12に駐在している時間の長さを所望の長さとすることができる。その結果、エージェントプログラム10が認証局12から末端エンティティ14に戻ってくるタイミングを所望のタイミングとすることができる。このため、CRLの更新を所望のタイミングで行なうことができる。

【0060】次に、末端CPU22によってエージェントプログラム10を実行することにより、エージェントプログラム10自身は、認証局12にオープンネットワークシステムを介して送られて、認証局メモリ18に格納される（図1の（B））。すなわち、エージェントプログラム10は、自身のプログラムに従って認証局メモリ（CAメモリ）18へ移動する（図2のS3）。

【0061】次に、認証局CPU16によってエージェントプログラム10を実行することにより、認証局メモリ18のうちのこのエージェントプログラム10が使用するメモリ領域に、認証局の発行している最新のCRLを格納する（図1の（B））。ここでは、このメモリ領域のCRL読み込みファイル10aに、第1CRLファイル20から最新CRLとして「CRL2」を読み込む（図2のS4）。尚、図1の（B）においては、エージェント10のCRL読み込みファイル10aに「CRL2」が読み込まれた状態を示す。

【0062】次に、エージェントプログラム10は、一定時間、認証局メモリ18に駐在する。駐在している間、認証局CPU16によって、エージェントプログラム10を実行することにより、経過時間を計測する。また、駐在している間、認証局CPU16によって、エージェントプログラム10を実行することにより、第1CRLファイル20の内容の更新状況を監視する。監視にあたっては、例えば、第1CRLファイル20のファイルの更新日時やファイルのバージョンを調べるとすると良い。そして、駐在している間に最新CRL20の内容が更新された場合は、更新された新しいCRLをCRL読み込みファイル10aに読み込む（図2のS5）。

【0063】また、図2において、太線の枠で示したS5およびS6のステップの処理は、認証局CPU16がエージェントプログラム10を実行することによって行われる。また、S5およびS6のステップ以外の処理（細線の枠で示されたステップS1～S4およびS7）の処理は、末端CPU22がエージェントプログラム10を実行することによって行われる。

【0064】次に、認証局CPU16によってエージェントプログラム10を実行することにより、一定時間の経過後に、エージェントプログラム10をメモリ領域に格納された第1CRLファイル20（その内容は「CRL2」である。）と共に、オープンネットワークシステムを介して送って末端メモリ24に格納する（図1の（C））。すなわち、エージェントプログラム10は、自身のプログラムに従って、CRL読み込みファイル10aを携えて、末端メモリ（EEメモリ）24に移動する（図2のS6）。

【0065】次に、末端メモリ24に格納されたエージェントプログラム10は、末端CPU22によって実行される。その結果、エージェントプログラム10の処理手順に従って、末端メモリ24に格納されている第2C



RLファイル(更新前の内容は「CRL1」である。)26の内容は、エージェントプログラム10が認証局のコンピュータ12から持ち帰った最新のCRLである「CRL2」に更新される(図2のS7)。尚、図1の(C)においては、第2CRLファイル26の内容が「CRL1」から「CRL2」に更新された状態を示す。このようにして、エージェントプログラム10により認証局12から末端エンティティ14へCRLが配布される。

【0066】このように、第1の実施の形態のCRLの配布方法によれば、CRLを配布するための処理手順がプログラムされたエージェントプログラム10を用いる。その結果、アプリケーションシステムとCRLの配布とを切り離すことができる。このため、アプリケーションシステムの設計をCRLの配布の仕組みの設計から切り離して行うことができる。このため、アプリケーションシステムの設計の負担を軽減することができる。

【0067】[第2の実施の形態]次に、第2の実施の形態では、図3および図4を参照して、この発明の第2の無効デジタル証明書リスト(CRL)の配布方法の一例について説明する。

【0068】図3の(A)~(C)は、第2の実施の形態のCRLの配布方法の説明に供するブロック図である。また、図4は、第1の実施の形態のCRLの配布方法の説明に供するフローチャートである。

【0069】また、通常は、認証局から多数の末端エンティティへCRLが配布されるが、第2の実施の形態では、第1の実施の形態と同様に、1つの末端エンティティおよび認証局に注目してCRLの配布方法について説明する。

【0070】また、CRLを配布するための処理手順がプログラムされたエージェントプログラム(以下、単に「エージェント」とも称する。)30が稼働する環境には、起動前のエージェント30が認証局のコンピュータの認証局メモリにコンパイルされて格納されている点を除いては、上述した第1の実施の形態における環境と同一である。従って、図1に示された環境の成分と同一の環境の成分については図3において同一の符号を付し、その詳細な説明を省略する。

【0071】次に、第2の実施の形態におけるCRLの配布方法について説明する。

【0072】CRLの配布を行うにあたり、まず、認証局メモリ18に格納されていたエージェントプログラム30を認証局CPU16によって起動する(図4のS1)。すなわち、認証局CPU16によってエージェントプログラム30の実行を開始する。起動にあたっては、例えば、認証局メモリ18中に格納されているローカルな関数の呼び出しを認証局CPU16によって行うことによって、エージェント30の実行を開始させると良い。

【0073】次に、認証局CPU16によってエージェントプログラム30を実行することにより、認証局メモリ18のうちのこのエージェントプログラム30が使用するメモリ領域に、認証局の発行している最新の無効デジタル証明書リスト(CRL)が格納される(図4のS2)。ここでは、第1CRLファイル20からメモリ領域のCRL読み込みファイル30aに、最新CRLとして「CRL2」を読み込む(図3の(A))。図3の(A)においては、エージェント30のCRL読み込みファイル30aに、「CRL2」が読み込まれた状態を示す。

【0074】次に、認証局CPU16によってエージェントプログラム30を実行することにより、エージェントプログラム30自身を、CRL読み込みファイル30aに格納された最新のCRL(「CRL2」)と共に、末端エンティティ14へオープンネットワークシステムを介して送って、末端メモリ(EEメモリ)24に格納する(図4のS3)。すなわち、エージェントプログラム30は、自身のプログラムに従って、末端エンティティ14へ移動する(図3の(B))。

【0075】次に、末端メモリ24に格納されたエージェントプログラム30は、末端CPU22によって実行される。その結果、エージェントプログラム30の処理手順に従って、当該末端メモリ24に格納されている第2CRLファイル26の内容が、CRL読み込みファイル30aの内容に更新される(図4のS4)。ここでは、第2CRLファイル26の内容「CRL1」から「CRL2」に更新する。このようにして、エージェントプログラム30により認証局から末端エンティティへ最新のCRLが配布される(図3の(B))。

【0076】尚、図3の(B)においては、第2CRLファイル26の内容が、「CRL1」から「CRL2」に更新された状態を示す。また、図4において、太線の枠で示したS4およびS5のステップの処理は、末端CPU22がエージェントプログラム30を実行することによって行われる。また、S4およびS5のステップ以外の処理(細線の枠で示されたステップS1~S3およびS5)の処理は、認証局CPU16がエージェントプログラム30を実行することによって行われる。

【0077】次に、エージェントプログラム30は、認証局CPU16によってエージェントプログラム30が実行されることにより、認証局メモリ(CAメモリ)18に、オープンネットワークシステムを介して送られて格納される(図4のS5)。すなわち、エージェントプログラムは、自身のプログラムに従って、認証局メモリ18に移動する(図3の(C))。

【0078】そして、認証局に戻ったエージェントプログラム30は、認証局CPU16に対して、CRLの配布が完了したことを報告する。

【0079】尚、第2の実施の形態においては、1つの

末端エンティティへCRLを配布する例について説明したが、この発明の第2のCRLの配布方法では、複数の末端エンティティへCRLを配布することも十分可能である。

【0080】その場合、例えば1つのエージェントが、1つの末端エンティティへCRLを配布した後、認証局へ戻らずに、複数の末端エンティティへCRLを順次に配布し、最後に認証局に戻っても良い。すなわち、図4に示したフローチャートにおいて、S3およびS4のステップを繰返しても良い。

【0081】そして、エージェントが複数の末端エンティティに順次にCRLを配布した場合には、認証局への完了報告に、例えば、実際にCRLを配布した末端エンティティの一覧を含めると良い。そして、認証局CPUに、末端エンティティの一覧に含まれていない末端エンティティ、すなわち、接続不能や末端メモリの容量不足のためにCRLの配布ができなかった末端エンティティを認証局CPUに把握させても良い。さらに、CRLの配布ができなかった末端エンティティに対してだけ、再びCRLの配布を試みても良い。

【0082】また、この発明の第2のCRLの配布方法によれば、例えば、複数のエージェントを同時に実行させても良い。

【0083】このように、第2の実施の形態のCRLの配布方法によれば、エージェントプログラム30を用いる。そして、このエージェントプログラム30にCRLの配布の仕組みの処理手順を設計する。その結果、アプリケーションシステムの設計をCRLの配布の仕組みの設計から切り離して行うことができる。このため、アプリケーションシステムの設計の負担を軽減することができる。

【0084】さらに、第2の実施の形態のCRLの配布方法によれば、認証局CPU16によって、エージェントプログラム30を起動して、エージェントプログラム30を末端メモリ24へ移動させる。その結果、多数の末端エンティティへCRLを配布する場合でも、認証局12へ末端エンティティからエージェントプログラムが殺到することがない。このため、認証局のコンピュータ12の負担の増大を抑制することができる。よって、特に認証局のコンピュータ12の処理能力に余裕がない場合に適用して好適である。

【0085】【第3の実施の形態】第3の実施の形態では、図5、図6および図7を参照して、この発明の第3の無効デジタル証明書リスト(CRL)の配布方法の一例について説明する。

【0086】図5の(A)～(C)および図6の(A)～(C)は、第3の実施の形態のCRLの配布方法の説明に供するブロック図である。また、図7は、第3の実施の形態のCRLの配布方法の説明に供するフローチャートである。

【0087】まず、1つの認証局から他の認証局へCRLを配布するための処理手順がプログラムされたエージェントプログラム(以下、単に「エージェント」とも称する。)が稼働する環境について説明する。通常は、多数の認証局どうしの間でCRLが互いに配布されるが、ここでは、第1認証局および第2認証局に注目してCRLの配布方法について説明する。

【0088】図5および図6には、第1認証局のコンピュータ(「第1CAコンピュータ」または「第1認証局」とも称する。)32と、第2認証局のコンピュータ(「第2CAコンピュータ」または「第2認証局」とも表記する。)34を示す。第1認証局32と第2認証局34とは、互いにオープンネットワークシステムによって接続してある。また、第1認証局32および第2認証局34は、いずれも、第1認証局32の発行するCRLを配布する第1エージェント36および第2認証局34の発行するCRLを配布する第2エージェント38が動作可能な環境を有している。動作可能な環境とは、例えば、第1認証局32と第2認証局34との間で第1および第2エージェント36および38のそれぞれの受渡が可能な状態をいう。

【0089】また、第1認証局32は、第1認証局CPU40および第1認証局メモリ42を具えている。この第1認証局メモリ42には、この第1認証局のコンピュータ32が発行した最新の無効デジタル証明書リスト(CRL)を内容とする第1CRLファイル44が格納されている。図5の(A)においては、第1CRLファイル44に、最新のCRLとして「CRL2」が格納された状態を示す。

【0090】また、この第1認証局メモリ42には、第2認証局のコンピュータ34から配布されたCRLを内容とする第2CRLファイル46が格納されている。また、図5の(A)においては、この実施の形態におけるCRLの配布前の状態として、第2CRLファイル46に「CRL3」が格納されている状態を示す。

【0091】そして、第1認証局メモリ42には、第1エージェントプログラム36がコンパイルされた状態で格納してある(図5の(A))。尚、図6の(A)～(C)では、第1エージェントプログラム36の図示を省略する。

【0092】また、第2認証局34は、第2認証局CPU48および第2認証局メモリ50を具えている。この第2認証局メモリ50には、この第2認証局のコンピュータ34が発行した最新のCRLを内容とする第3CRLファイル52が格納されている。第3の実施の形態においては、第3CRLファイル52に最新のCRLとして「CRL4」が格納されている。

【0093】また、この第2認証局メモリ50には、第1認証局のコンピュータ32から配布されたCRLを内容とする第4CRLファイル54が格納されている。図

5の(A)においては、この実施の形態で説明するCRLの配布前の状態として、第4CRLファイル54に「CRL1」が格納されている状態を示す。

【0094】そして、第2認証局メモリ50には、第2エージェントプログラム38がコンパイルされた状態で格納してある。尚、図5の(A)～(C)では、第2エージェントプログラム38の図示を省略してある。

【0095】次に、第3の実施の形態におけるCRLの配布方法について説明する。ここでは、第1認証局のコンピュータ32から第2認証局のコンピュータ34へCRLを配布した後、第2認証局のコンピュータ34から第1認証局のコンピュータ32へCRLを配布する例について説明する。

【0096】まず、第1認証局32から第2認証局34へのCRLの配布を行うにあたり、第1認証局メモリ42に格納されていた第1エージェントプログラム36を第1認証局CPU40によって起動する(図7のS1)。すなわち、第1認証局CPU40によって第1エージェントプログラム36の実行を開始する。起動にあたっては、例えば、第1認証局メモリ42中に格納されているローカルな関数の呼び出しを第1認証局CPU40によって行うことによって、第1エージェントプログラム36の実行を開始させると良い。

【0097】次に、第1認証局CPU40によって第1エージェントプログラム36を実行することにより、認証局メモリ42のうちのこの第1エージェントプログラム36が使用するメモリ領域に、第1認証局の発行している最新の無効デジタル証明書リスト(CRL)を格納する(図7のS2)。ここでは、このメモリ領域のCRL読み込みファイル36aに、第1CRLファイル44から最新CRLとして「CRL2」を読み込む(図5の(A))。図5の(A)においては、CRL読み込みファイル36aに、「CRL2」が読み込まれた状態を示す。

【0098】次に、第1認証局CPU40によって第1エージェントプログラム36を実行することにより、第1エージェントプログラム36自身を、CRL読み込みファイル36aに格納された最新のCRLである「CRL2」と共に、第2認証局34へオープンネットワークシステムを介して送って、第2認証局メモリ50に格納する(図5の(B))。すなわち、第1エージェントプログラム36は、自身のプログラムに従って、第2認証局(第2CA)34へ移動する(図7のS3)。

【0099】次に、第2認証局メモリ50に格納された第1エージェントプログラム36は、第2認証局CPU48によって実行される。その結果、第1エージェントプログラム36の処理手順に従って、第2認証局メモリ50の第4CRLファイル54に格納されている古いCRL(ここでは「CRL1」)が、最新のCRL(「CRL2」)に更新される(図7のS4)。このようにし

て、第1エージェントプログラム36によって第1認証局32から第2認証局34へ最新のCRL(「CRL2」)が配布される(図5の(B))。

【0100】尚、図5の(B)においては、第4CRLファイル54の内容が「CRL2」に更新される前の状態を示す。また、図7において細線の枠で示したS1～S3のステップの処理は、前述したように、第1認証局CPU40が第1エージェントプログラム36を実行することによって行われる。これに対して、太線の枠で示したS4～S5のステップの処理は、第2認証局CPU48が第1エージェントプログラム36を実行することによって行われる。また、図7において太線の枠で示したS6～S8のステップの処理は、第2認証局CPU48が第2エージェントプログラム38を実行することによって行われる。これに対して、細線の枠で示されたS9およびS10のステップの処理は、第1認証局CPU40が第2エージェントプログラム38を実行することによって行われる。

【0101】次に、第1エージェントプログラム36は、第2認証局CPU48によって第1エージェントプログラム36が実行されることにより、第1認証局32にオープンネットワークシステムを介して送られて、第1認証局メモリ42格納される(図5の(C))。すなわち、エージェントプログラム36は、自身のプログラムに従って、第1認証局(第1CA)32に移動する(図7のS5)。

【0102】そして、第1認証局32に戻った第1エージェントプログラム36は、第1認証局CPU40に対して、CRLの配布が完了したことを報告する。

【0103】次に、第2認証局34から第1認証局32へのCRLの配布を行うにあたり、第2認証局メモリ50に格納されていた第2エージェントプログラム38を第2認証局CPU48によって起動する(図7のS6)。すなわち、第2認証局CPU48によって第2エージェントプログラム38の実行を開始する。起動にあたっては、例えば、第2認証局メモリ50中に格納されているローカルな関数の呼び出しを第2認証局CPU48によって行うことによって、第2エージェントプログラム38の実行を開始させると良い。

【0104】次に、第2認証局CPU48によって第2エージェントプログラム38を実行することにより、第2認証局メモリ50のうちのこの第2エージェントプログラム38が使用するメモリ領域に、第2認証局34の発行している最新の無効デジタル証明書リスト(CRL)を格納する(図7のS7)。ここでは、このメモリ領域のCRL読み込みファイル38aに、第3CRLファイル52から最新CRLとして「CRL4」を読み込む(図6の(A))。図6の(A)においては、CRL読み込みファイル38aに、「CRL4」が読み込まれた状態を示す。

【0105】次に、第2認証局CPU48によって第2エージェントプログラム38を実行することにより、第2エージェントプログラム38自身を、CRL読み込みファイル36aに格納された最新のCRLである「CRL4」と共に、第1認証局32へオープンネットワークシステムを介して送って、第1認証局メモリ42に格納する(図6の(B))。即ち、第2エージェントプログラム38は、自身のプログラムに従って、第1認証局(第1CA)32へ移動する(図7のS8)。

【0106】次に、第1認証局メモリ42に格納された第2エージェントプログラム38は、第1認証局CPU40によって実行される。その結果、第2エージェントプログラム38の処理手順に従って、第1認証局メモリ42の第2CRLファイル46に格納されている古いCRL(ここでは「CRL3」)が、最新のCRL(「CRL4」)に更新される(図7のS9)。このようにして、第2エージェントプログラム38によって第2認証局34から第1認証局32へ最新のCRL(「CRL4」)が配布される(図6の(B))。尚、図6の(B)においては、第2CRLファイル46の内容が「CRL4」に更新される前の状態を示す。

【0107】次に、第2エージェントプログラム38は、第1認証局CPU40によって第2エージェントプログラム38が実行されることにより、第2認証局34にオープンネットワークシステムを介して送られて、第2認証局メモリ50に格納される(図6の(C))。すなわち、エージェントプログラム36は、自身のプログラムに従って、第2認証局(第2CA)34に移動する(図7のS10)。

【0108】そして、第2認証局34に戻った第2エージェントプログラム38は、第2認証局CPU48に対して、CRLの配布が完了したことを報告する。

【0109】このように、第3の実施の形態の無効デジタル証明書リストの配布方法によれば、第1および第2エージェントプログラム36および38を用いる。そして、この第1および第2エージェントプログラム36および38のそれぞれにCRLの配布の仕組みの処理手順を設計する。その結果、個々の認証局32および34のシステムの設計をCRLの配布の仕組みの設計から切り離して行うことができる。このため、第1および第2認証局32および34のシステムの設計の負担を軽減することができる。

【0110】また、第3の実施の形態においては、第1認証局32と第2認証局34との間でCRLを配布する場合について説明したが、この発明の第3のCRLの配布方法によれば、3つ以上の認証局どうしの間でCRLを互いに配布することも可能である。

【0111】また、第3の実施の形態においては、第1認証局から第2認証局へCRLを配布した後に、第2認証局から第1認証局へCRLを配布したが、この発明の

第3のCRLの配布方法では、CRLの配布の順序は限定されない。例えば、第1認証局と第2認証局との間のCRLの配布を同時に行っても良い。より具体的には、例えば、図7に示す各ステップをS1、S6、S2、S7、S3、S8、S9、S10の順序で実行しても良い。

【0112】

【発明の効果】

【第1の無効デジタル証明書リストの配布方法について】この発明の第1の無効デジタル証明書リストの配布方法によれば、エージェントプログラムを用いる。そして、このエージェントプログラムにCRLの配布の仕組みの処理手順を設計する。その結果、アプリケーションシステムの設計をCRLの配布の仕組みの設計から切り離して行うことができる。このため、アプリケーションシステムの設計の負担を軽減することができる。

【0113】また、この発明の第1の無効デジタル証明書リストの配布方法を実施するにあたり、エージェントを認証局に駐在させる一定時間を設定して末端メモリに格納しておき、これをエージェントプログラムに読み込ませて設定すれば、エージェントプログラムが認証局に駐在している時間の長さを所望の長さとすることができる。その結果、エージェントプログラムが認証局から末端エンティティに戻ってくるタイミングを所望のタイミングとすることができる。このため、CRLの更新のタイミングを所望のタイミングとすることができる。

【0114】【第2の無効デジタル証明書リストの配布方法について】また、この発明の第2の無効デジタル証明書リストの配布方法によれば、エージェントプログラムを用いる。そして、このエージェントプログラムにCRLの配布の仕組みの処理手順を設計する。その結果、アプリケーションシステムの設計をCRLの配布の仕組みの設計から切り離して行うことができる。このため、アプリケーションシステムの設計の負担を軽減することができる。

【0115】さらに、この発明の第2の無効デジタル証明書リストの配布方法によれば、認証局CPUによって、エージェントプログラムを起動して、エージェントプログラムを末端メモリへ移動させる。このため、第2の無効デジタル証明書リストの配布方法によれば、認証局へ末端エンティティからエージェントプログラムが殺到することがない。その結果、認証局のコンピュータの負担の増大を抑制することができる。従って、第2の無効デジタル証明書リストの配布方法は、特に認証局のコンピュータの処理能力に余裕がない場合に適用して好適である。

【0116】【第3の無効デジタル証明書リストの配布方法について】また、この発明の第3の無効デジタル証明書リストの配布方法によれば、エージェントプログラムを用いる。そして、このエージェントプログラム

10

20

30

40

50

にCRLの配布の仕組みの処理手順を設計する。その結果、個々の認証局のシステムの設計をCRLの配布の仕組みの設計から切り離して行うことができる。このため、認証局のシステムの設計の負担を軽減することができる。

【図面の簡単な説明】

【図1】第1の実施の形態の無効デジタル証明書リストの配布方法の説明に供するブロック図である。

【図2】第1の実施の形態の無効デジタル証明書リストの配布方法の説明に供するフローチャートである。

【図3】第2の実施の形態の無効デジタル証明書リストの配布方法の説明に供するブロック図である。

【図4】第2の実施の形態の無効デジタル証明書リストの配布方法の説明に供するフローチャートである。

【図5】第3の実施の形態の無効デジタル証明書リストの配布方法の説明に供する前半のブロック図である。

【図6】第3の実施の形態の無効デジタル証明書リストの配布方法の説明に供する後半のブロック図である。

【図7】第3の実施の形態の無効デジタル証明書リストの配布方法の説明に供するフローチャートである。

【符号の説明】

10 : エージェントプログラム

10a : CRL読み込みファイル

12 : 認証局のコンピュータ (認証局)

14 : 末端エンティティのコンピュータ (末端エンティティ)

ティ)

16 : 認証局CPU

18 : 認証局メモリ

20 : 第1CRLファイル

22 : 末端CPU

24 : 末端メモリ

26 : 第2CRLファイル

28 : 一定時間を設定したファイル

30 : エージェントプログラム

10 30a : CRL読み込みファイル

32 : 第1認証局のコンピュータ (第1認証局)

34 : 第2認証局のコンピュータ (第2認証局)

36 : 第1エージェントプログラム

36a : CRL読み込みファイル

38 : 第2エージェントプログラム

38a : CRL読み込みファイル

40 : 第1認証局CPU

42 : 第1認証局メモリ

44 : 第1CRLファイル

20 46 : 第2CRLファイル

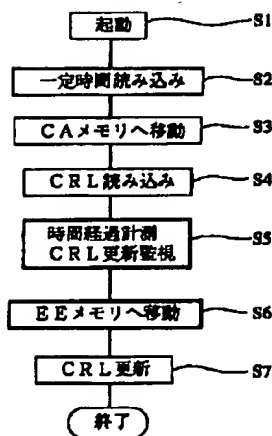
48 : 第2認証局CPU

50 : 第2認証局メモリ

52 : 第3CRLファイル

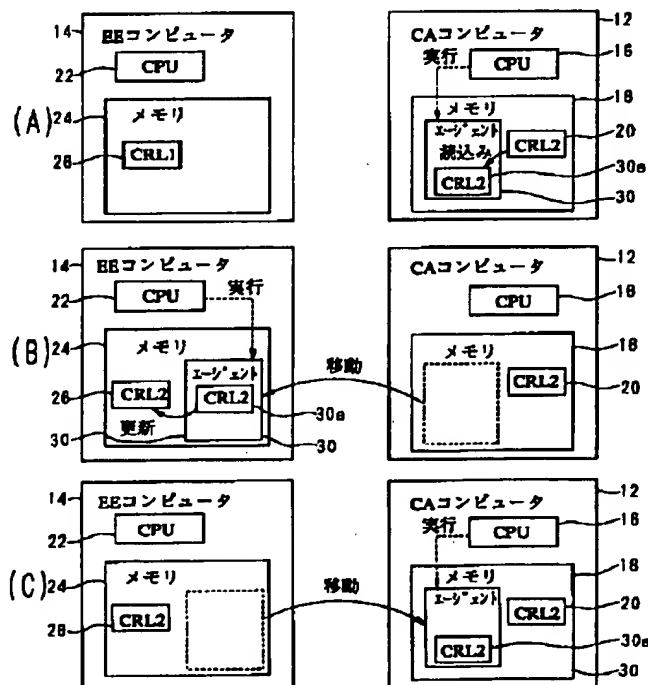
54 : 第4CRLファイル

【図2】



第1の実施の形態のフローチャート

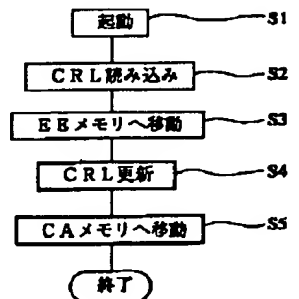
【図3】



30 : エージェントプログラム      30a : CRL読み込みファイル

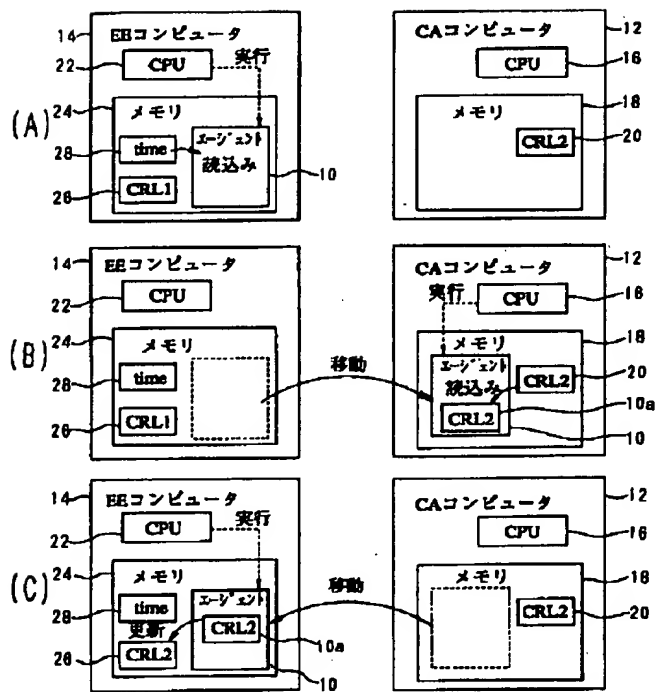
第2の実施の形態のブロック図

【図4】



第2の実施の形態のフローチャート

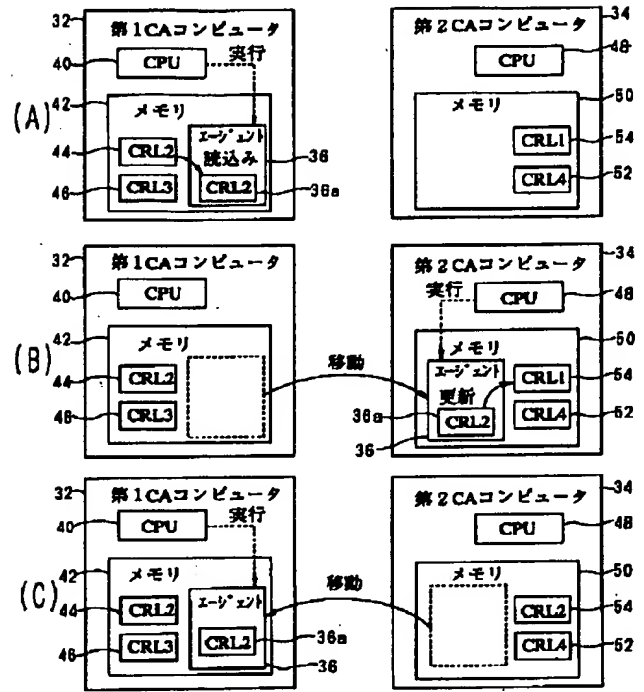
【図1】



10: エージェントプログラム  
 12: 認証局のコンピュータ  
 16: 認証局CPU  
 20: 第1 CRL ファイル  
 24: 末端メモリ  
 28: 一定時間を設定したファイル  
 10a: CRL読み込みファイル  
 14: 末端エンティティのコンピュータ  
 18: 認証局メモリ  
 22: 末端CPU  
 26: 第2 CRL ファイル

第1の実施の形態のブロック図

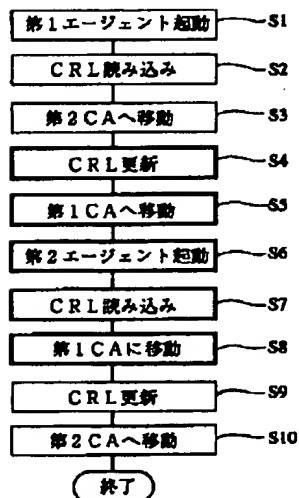
【図5】



32: 第1 認証局のコンピュータ  
 36: 第1 エージェントプログラム  
 40: 第1 認証局CPU  
 44: 第1 CRL ファイル  
 46: 第2 認証局CPU  
 52: 第3 CRL ファイル  
 34: 第2 認証局のコンピュータ  
 36a: CRL読み込みファイル  
 42: 第1 認証局メモリ  
 48: 第2 CRL ファイル  
 50: 第2 認証局メモリ  
 54: 第4 CRL ファイル

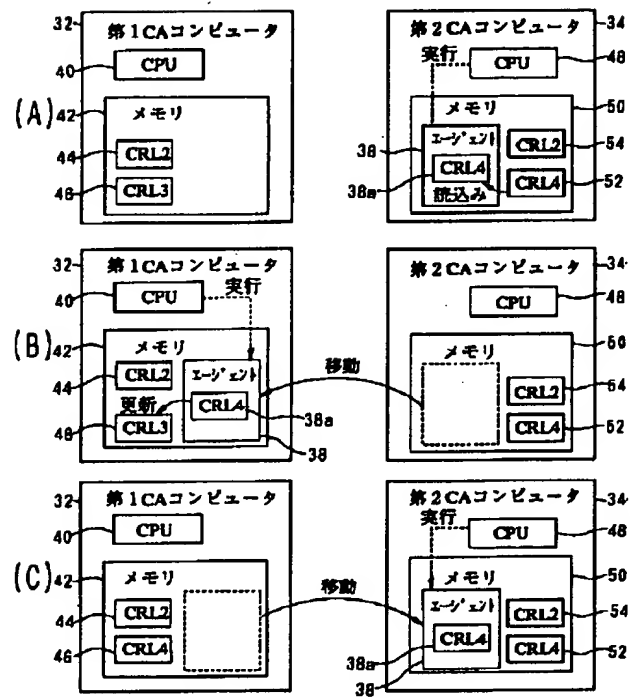
第3の実施の形態のブロック図（前半）

【図7】



第3の実施の形態のフローチャート

【図6】



38: 第2エージェントプログラム      38a: CRL読み込みファイル

第3の実施の形態のブロック図 (後半)